CHAPTER 5

ADVANCED ENCRYPTION STANDARD (AES)

LEARNING OBJECTIVES

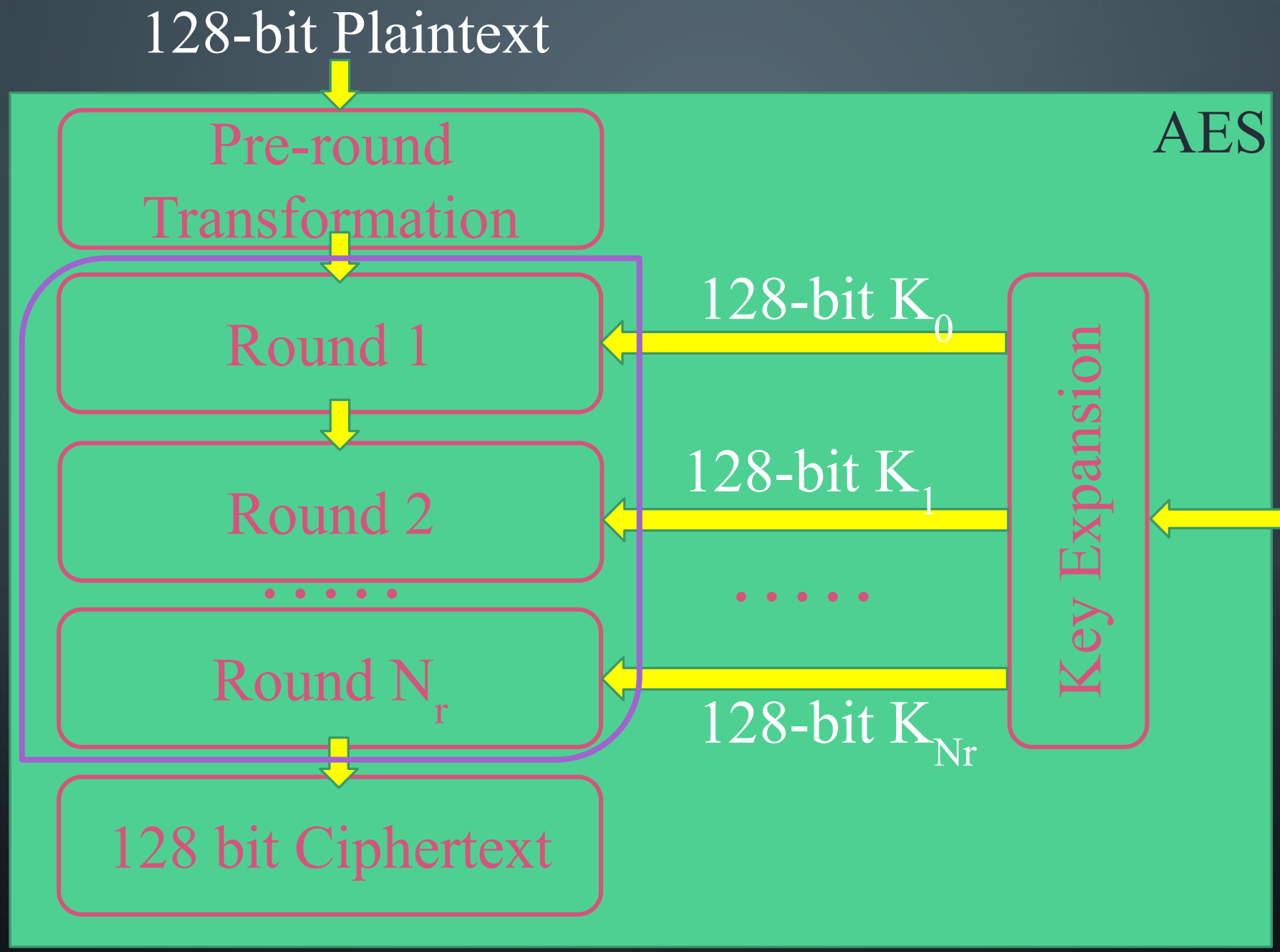
- To review a short history of AES
- To define the basic structure of AES
- To describe the transformation of AES
- To define the key expansion process
- To discuss different implementations

INTRODUCTION

- DES is symmetric key block cipher published by the National Institute of Standards and Technology (NIST)
- 1997 – NIST started looking for replacement for DES
- Required specification – 128 bits block size & 3 different key sizes 128, 192, and 256 bits
- NIST announced Rijndeal, designed by Belgian researchers Joan Daemen and Vincent Rijnment was selected as AES
- AES finally publish as FIPS 197 – December 2001

CRITERIA

- Security :
  - ✔ 128 bit key
- Cost :
  - ✔ computational efficiency and storage requirement for different implementation such as hardware, software, or smart cards
- Implementation :
  - ✔ flexibility and simplicity



N_r	Key Size
10	128
12	192
14	256

DATA UNITS

- Bit :
  - ✔ Binary digit with value of 0 & 1
  - ✔ Use lowercase letter to refer to a bit
- Byte :
  - ✔ Group of 8 bits that can be treated as single entity
  - ✔ Use lowercase bold letter to refer to a byte
- Word :
  - ✔ Group of 32 bits that can be treated as single entity
  - ✔ Use lowercase letter w to show a word

Continue .....

- Block :
  - ✔ Group of 128 bits
  - ✔ Use lowercase letter to refer to a bit

- State :
  - ✔ AES uses several rounds in which each round is made of several stages.
  - ✔ At beginning and end of the cipher, AES uses the term data block; before and after each stage, data block is referred to as a state
  - ✔ Use uppercase bold letter to refer to a state

EXAMPLE:

GIVEN TEXT BLOCK IS:“AES USES A MATRIX”

REPRESENT IT IN THE FORM OF STATE.

ANSWER:
GIVEN TEXT BLOCK IS: “AES USES A MATRIX”

As we know that state is made up of 128 bits i.e. 16 bytes.
So calculate the number of characters. If it is 16 then it is the complete block but if it is not then add padding

A E S U S E S A M A T R I X Z Z

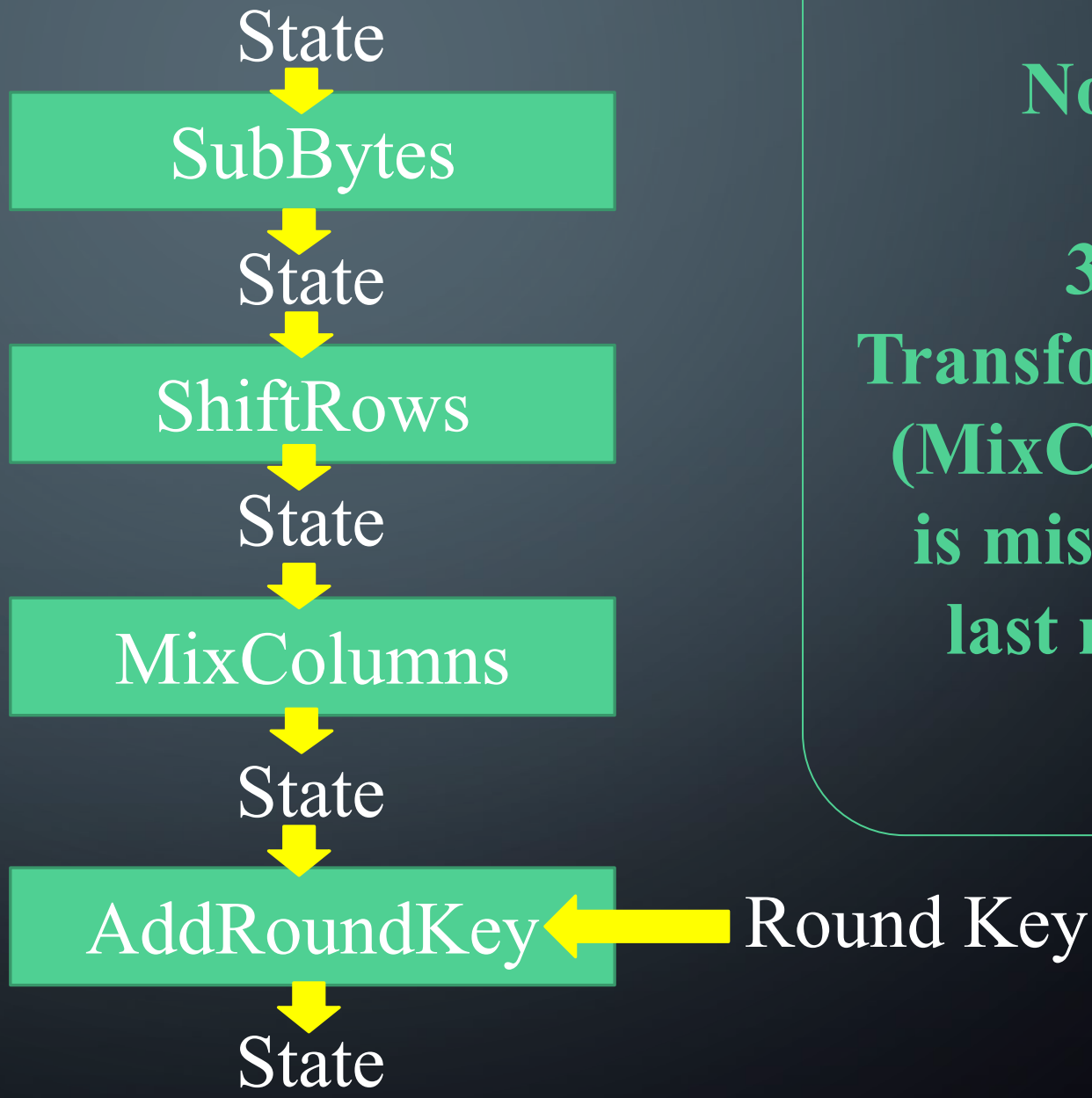
NOW WRITE THE Hexadecimal values of each character

00 04 12 14 12 04 12 00 0C 00 13 11 08 23 19 19

Arrange all the values in 4 X 4 matrix

00	12	0C	08
04	04	00	23
12	12	13	19
14	00	11	13

STRUCTURE OF EACH ROUND



Note:

One Add Round Key is applied before first round

Note:

3rd Transformation (MixColumn) is missing in last round

TRANSFORMATION

- ✔ To provide security, AES uses four types of transformations

1. Substitution : SubBytes
2. Permutation : ShiftRows
3. Mixing : MixColumns
4. Key adding : AddRoundKey

Continue .....

Substitution :

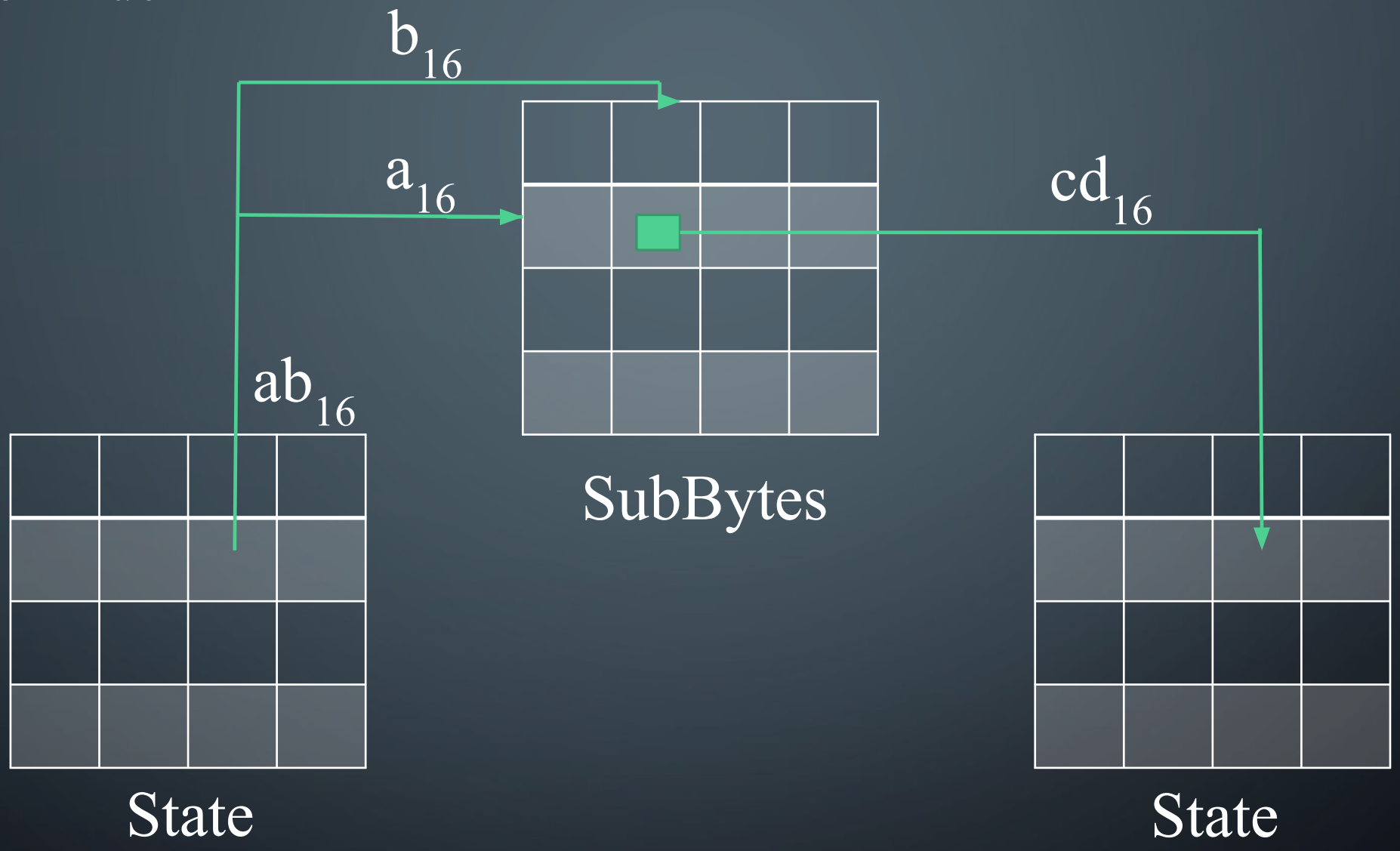
- ✔ First - substitution is done for each byte
- ✔ Second – only one table is used for transformation of every byte
- ✔ Third – transformation is defined by either table lookup process or mathematical calculation

SubBytes:

To substitute a byte, interpret byte as two hexadecimal digits

Left digit – row & right digit - column

Continue .....



Continue .....

SubBytes Transformation Table

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79

Continue .....

Example:

Apply SubByte Transformation on below state

$$\begin{pmatrix} 00 & 12 & 0C & 08 \\ 04 & 04 & 00 & 23 \\ 12 & 12 & 13 & 19 \\ 14 & 00 & 11 & 13 \end{pmatrix}$$

Continue .....

Answer:

63	C9	FE	30
F2	F2	63	26
C9	C9	7D	D4
FA	63	82	D4

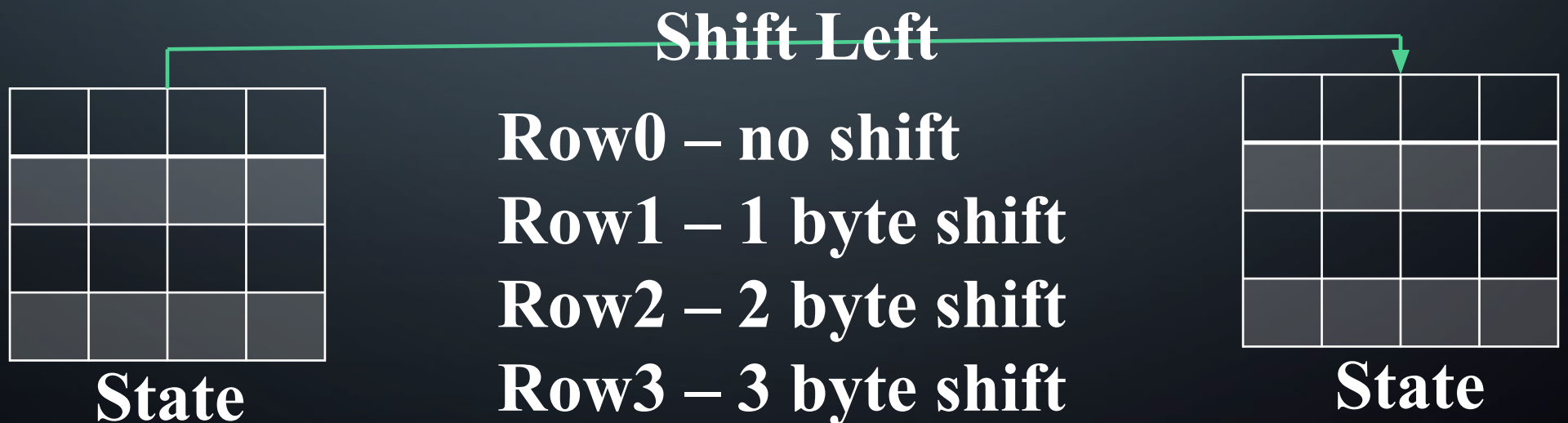
Continue .....

Permutation :

- ✔ Permutes bytes
- ✔ Order of bits in byte is not changed

❖ ShiftRows :

- ✔ Shift left (circular)
- ✔ No byte shifting, depends on row number
- ✔ Row 0 - no shifting, row 1 – shift 1 byte, so on



Continue .....

Mixing :

- ✔ Changes the content of each byte by taking 4 bytes at a time and combining them to recreate 4 new bytes
- ✔ Matrix multiplication – square matrix X column matrix

- ❖ **MixColumns :**

  - ✔ Operates at column level
  - ✔ Multiplication of Constant square matrix and state column

Continue .....

Key Adding :

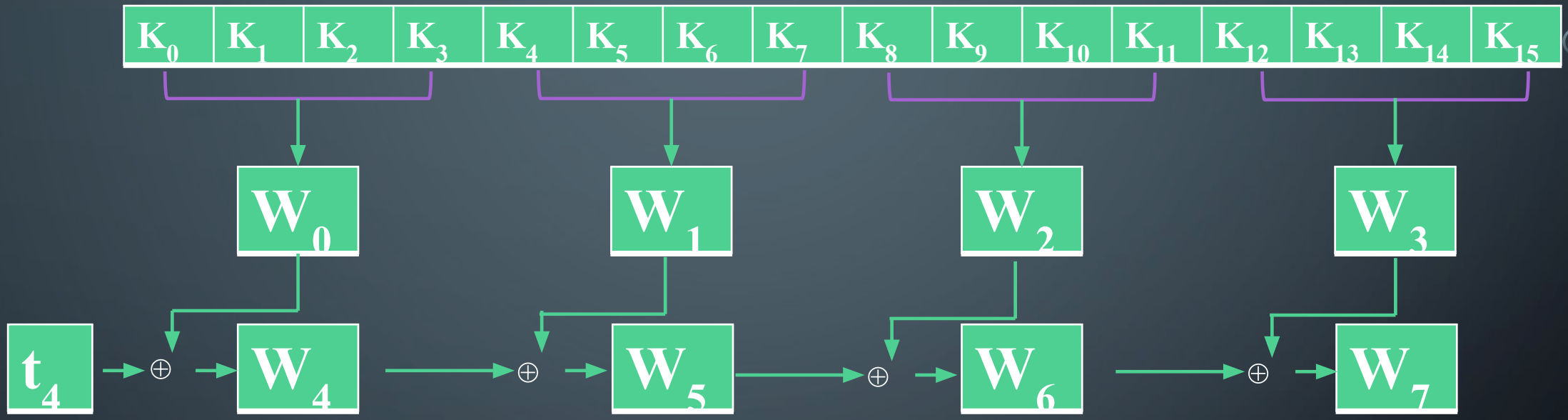
- ✔ AES uses a process called key expansion that creates $N_r + 1$ round key
- ✔ Each round key is 128 bits long – 4 32-bit words
- ✔ Each word is considered as column matrix

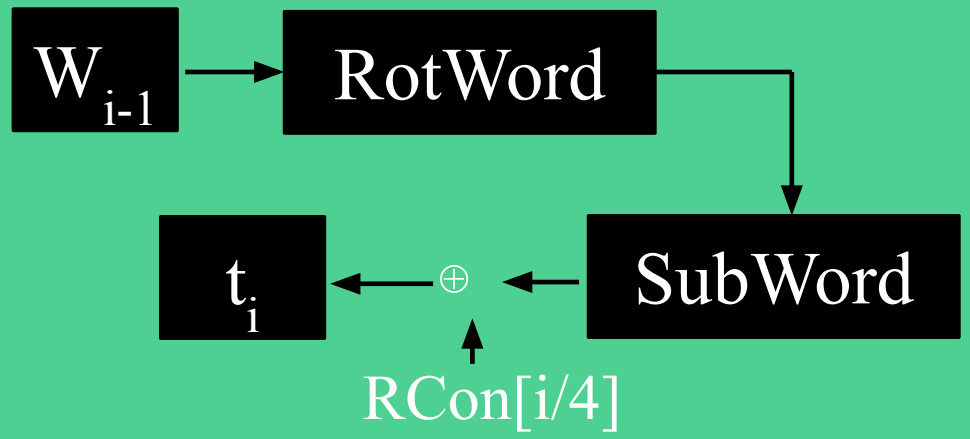
- ❖ **AddRoundKey :**

  - ✔ Adds a round key word with each state column matrix
  - ✔ Matrix addition

Continue .....

Key Expansion





Note:

AES-128	10 Rounds 44 Words
AES-192	12 Rounds 52 Words
AES-256	14 Rounds 60 Words

Continue .....

Round Constants :

Round	Constant	Round	Constant
1	01 00 00 00	6	20 00 00 00
2	02 00 00 00	7	40 00 00 00
3	04 00 00 00	8	80 00 00 00
4	08 00 00 00	9	1B 00 00 00
5	10 00 00 00	10	36 00 00 00

Continue .....

ANALYSIS OF AES

- Security
  - ✔ Brute-force Attack
  - ✔ Statistical Attack
  - ✔ Differential and Linear Attacks
- Implementation
- Simplicity and Cost

REFERENCE BOOK:

CRYPTOGRAPHY AND NETWORK SECURITY – BEHROUZ A FOROUZAN, DEBDEEP MUKHOPADHYAY